CLAIM LISTING

Amendments to the claims are reflected in the following listing, which replaces any and all prior versions and listings of claims in the present application:

Amendments to the Claims:

1. (Currently Amended) A transponder reader transaction system configured with a biometric security apparatus ~~system~~, said system comprising:

a transponder configured to communicate with a reader;

a reader configured to communicate with said system;

a keystroke scan sensor configured to detect a proffered keystroke scan sample, said keystroke scan sensor configured to communicate with said system; and,

a device configured to verify said proffered keystroke scan sample to facilitate a transaction, said device further configured to verify whether said proffered keystroke scan sample is associated with a preset transaction limitation independent of a financial account transaction limitation.

2. (Original) The transponder-reader transaction system of claim 1, wherein said sensor is configured to communicate with said system via at least one of a transponder, a reader, and a network.

3. (Currently Amended) The transponder-reader transaction system of claim 1, wherein said keystroke scan sensor is configured to facilitate a ~~finite~~ limited number of scans.

4. (Original) The transponder-reader transaction system of claim 1, wherein said keystroke scan sensor is configured to log at least one of a detected keystroke scan sample, processed keystroke scan sample and stored keystroke scan sample.

5. (Original) The transponder-reader transaction system of claim 1, further including a database configured to store at least one data packet, wherein said data packet includes at least one of proffered and registered keystroke scan samples, proffered and registered user information, terrorist information, and criminal information.

6. (Original) The transponder-reader transaction system of claim 4, wherein said database is contained in at least one of the transponder, transponder reader, sensor, remote server, merchant server and transponder-reader system.

7. (Currently Amended) The transponder-reader transaction system of claim 5, wherein said ~~remote~~ database is configured to be operated by an authorized sample receiver.

8. (Currently Amended) The transponder-reader transaction system of claim 1, wherein said keystroke scan sensor ~~device~~ is configured with at least one of an electronic sensor, an optical sensor and a keyboard.

9. (Original) The transponder-reader transaction system of claim 1, wherein said keystroke scan sensor is configured to detect and verify keystroke scan characteristics including at least one of behavioral, temporal and physical characteristics.

10. (Currently Amended) The transponder-reader transaction system of claim 1, wherein said keystroke scan sensor ~~device~~ is configured to detect false keystrokes and body heat.

11. (Original) The transponder-reader transaction system of claim 1, further including a device configured to compare a proffered keystroke scan sample with a stored keystroke scan sample.

12. (Currently Amended) The transponder-reader transaction system of claim 11, wherein said stored keystroke scan sample is stored by one of a third-party biometric security vendor and a governmental agency ~~device configured to compare a keystroke scan sample is at least one of a third-party security vender device and protocol/sequence controller~~.

13. (Original) The transponder reader transaction system of claim 11, wherein a stored keystroke scan sample comprises a registered keystroke scan sample.

14. (Original) The transponder-reader transaction system of claim 13, wherein said registered keystroke scan sample is associated with at least one of: personal information, credit card information, debit card information, savings account information, and loyalty point information.

15. (Original) The transponder-reader transaction system of claim 14, wherein different registered keystroke scan samples are associated with a different one of: personal information, credit card information, debit card information, savings account information, and loyalty point information.

16. (Currently Amended) The transponder-reader transaction system of claim 14, wherein a said registered keystroke scan sample is primarily associated with at least one of first user information, wherein said first information comprises personal information, credit card information, debit card information, savings account information, and loyalty point information.

and wherein a said registered keystroke scan sample is secondarily associated with at least one of second user information, wherein said second information comprises personal information, credit card information, debit card information, savings account information, and loyalty point information, where second user information is different than first user information.

17. (Original) The transponder-reader transaction system of claim 1, wherein said transponder-reader transaction system is configured to begin mutual authentication upon verification of said proffered keystroke scan sample.

18. (Original) The transponder-reader transaction system of claim 1, wherein said transponder is configured to deactivate upon rejection of said proffered keystroke scan sample.

19. (Original) The transponder-reader transaction system of claim 1, wherein said sensor is configured to provide a notification upon detection of a sample.

20. (Currently Amended) The transponder-reader transaction system of claim 1, wherein said device is further configured to ~~verify is configured to~~ facilitate at least one of access, activation of a second device, a financial transaction, and a non-financial transaction.

21. (Currently Amended) The transponder-reader transaction system of claim 1, wherein said device is further configured to ~~verify is configured to~~ facilitate the use of at least one secondary security procedure.

22. (Currently Amended) A method for facilitating biometric security in a transponder-reader transaction system comprising: proffering a keystroke scan sample to a keystroke scan sensor communicating with said system to initiate verification of a said keystroke scan sample for facilitating authorization of a transaction, said verification including determining whether said proffered keystroke scan sample is associated with a preset transaction limitation independent of a financial account transaction limitation.

23. (Currently Amended) The method ~~for~~ of claim 22, further comprising registering ~~at least one~~ a keystroke scan sample with an authorized sample receiver.

24. (Original) The method of claim 23, wherein said step of registering further includes at least one of: contacting said authorized sample receiver, proffering a keystroke scan to said authorized sample receiver, processing said keystroke scan sample ~~to obtain a keystroke scan sample~~, associating said keystroke scan sample with user information, verifying said keystroke scan sample, and storing said keystroke scan sample upon verification.

25. (Currently Amended) The method of claim 22, wherein said step of proffering includes proffering a keystroke scan sample to at least one of an electronic sensor, an optical sensor and a keyboard.

26. (Currently Amended) The method of claim 22, wherein said step of proffering further includes proffering a keystroke scan sample to a keystroke scan sensor communicating with said system to initiate at least one of storing, comparing, and verifying said keystroke scan sample.

27. (Currently Amended) The method of claim 22, ~~wherein said step of proffering a keystroke scan to a keystroke scan sensor communicating with said system to initiate verification further includes further~~ further comprising processing database information, wherein said database information is contained in at least one of a transponder, transponder reader, sensor, remote server, merchant server and transponder-reader system.

28. (Currently Amended) The method of claim 22, ~~wherein said step of proffering a keystroke scan sample to a keystroke scan sensor communicating with said system to initiate verification further includes~~ further comprising comparing a proffered keystroke scan sample with a stored keystroke scan sample.

29. (Original) The method of claim 28, wherein said step of comparing includes comparing a proffered keystroke scan sample to a stored keystroke scan sample stored by at least one of a third-party biometric security vendor and a governmental agency ~~by using at least one of a third-party security vendor device and protocol/sequence controller~~.

30. (Original) The method of claim 28, wherein said step of comparing includes comparing keystroke scan characteristics including at least one of behavioral, temporal and physical characteristics.

31. (Currently Amended) The method of claim 22, ~~wherein said step of proffering a keystroke scan to a keystroke scan sensor communicating with said system further comprises~~ further comprising using said keystroke scan sensor to detect at least one of false keystrokes and body heat.

32. (Currently Amended) The method of claim 22, ~~wherein said step of proffering a keystroke scan to a keystroke scan sensor communicating with said system to initiate verification further includes~~ further comprising at least one of detecting, processing and storing at least one second proffered keystroke scan sample.

33. (Currently Amended) The method of claim 22, ~~wherein said step of proffering a keystroke scan to a keystroke scan sensor communicating with said system to initiate verification further includes the use~~ of further comprising at least one secondary security procedure.

34. (Currently Amended) A method for facilitating biometric security in a transponder-reader transaction system comprising:

detecting a proffered keystroke scan sample at a sensor communicating with said system ~~to obtain a proffered keystroke scan sample~~;

verifying ~~the~~ said proffered keystroke scan sample including determining whether said proffered keystroke scan sample is associated with a preset transaction limitation independent of a financial account transaction limitation; and

authorizing a transaction to proceed upon verification of ~~the~~ said proffered keystroke scan sample.

35. (Currently Amended) The method of claim 34, wherein said step of detecting further includes detecting a proffered keystroke scan sample at a sensor configured to communicate with said system via at least one of a transponder, reader, and network.

36. (Currently Amended) The method of claim 34, wherein said step of detecting a said proffered keystroke scan sample includes detecting a proffered keystroke scan at least one of an electronic sensor, an optical sensor and a keyboard.

37. (Original) The method of claim 34, wherein said step of detecting includes at least one of: ~~detecting,~~ storing, and processing a said proffered keystroke scan sample.

38. (Currently Amended) The method of claim 34, wherein said step of detecting further includes receiving a ~~finite~~ limited number of proffered keystroke scan samples during a transaction.

39. (Currently Amended) The method of claim 34, ~~wherein said step of detecting further includes~~ further comprising logging each proffered keystroke scan sample.

40. (Currently Amended) The method of claim 34, ~~wherein said step of detecting further includes~~ further comprising at least one of detecting ~~detection~~, processing and storing ~~a at least one~~ second proffered keystroke scan sample.

41. (Original) The method of claim 34, wherein said step of detecting further includes using said keystroke scan sensor to detect at least one of false keystrokes and body heat.

42. (Currently Amended) The method of claim 34, wherein said step of verifying includes comparing a said proffered keystroke scan sample with a stored keystroke scan sample.

43. (Currently Amended) The method of claim 42, wherein said step of comparing a said proffered keystroke scan sample with a stored keystroke scan sample comprises storing, processing and comparing at least one of behavioral, temporal and physical characteristics.

44. (Currently Amended) The method of claim 42, wherein comparing a said proffered keystroke scan sample with a stored keystroke scan sample includes comparing a said proffered keystroke scan sample with at least one of a biometric sample of a criminal, a terrorist, and a transponder user.

45. (Currently Amended) The method of claim 34, wherein said step of verifying includes verifying a said proffered keystroke scan sample using information contained on at least one of a local database, a remote database, and a third-party controlled database.

46. (Currently Amended) The method of claim 34, wherein said step of verifying includes verifying a said proffered keystroke scan sample using one of a protocol/sequence controller and a third-party security vendor.

47. (New) The transponder-reader transaction system of claim 1, wherein said preset transaction limitation comprises at least one of a maximum transaction amount, minimum transaction amount, maximum number of transactions within a time period, maximum number of transactions, use by certain merchants, temporal limitation, geographic limitation, and use of non-monetary funds.

48. (New) The system of claim 1, wherein said device is further configured to require a second proffered biometric scan sample to override said preset transaction limitation.

49. (New) The transponder-reader transaction system of claim 16, wherein said first user account and said second user account are associated with different users.

50. (New) The method of claim 22, wherein said preset transaction limitation comprises at least one of a maximum transaction amount, minimum transaction amount, maximum number of transactions within a time period, maximum number of transactions, use by certain merchants, temporal limitation, geographic limitation, and use of non-monetary funds.

51. (New) The method of claim 22, wherein said device is further configured to require a second proffered biometric scan sample to override said preset transaction limitation.

52. (New) The method of claim 34, wherein said preset transaction limitation comprises at least one of a maximum transaction amount, minimum transaction amount, maximum number of transactions within a time period, maximum number of transactions, use by certain merchants, temporal limitation, geographic limitation, and use of non-monetary funds.

53. (New) The method of claim 34, wherein said device is further configured to require a second proffered biometric scan sample to override said preset transaction limitation.